

HOW IT WORKS

Digital rights management

DRM was meant to signal the end of music piracy, but there are serious questions over how it works or, indeed, if it works at all. Tom Royal considers the development and effectiveness of the most popular DRM systems

Digital rights management (DRM) has rarely been out of the news over the past year or so. The use of DRM in music-download services has become common, with services such as the iTunes Store and Napster selling and renting thousands of songs, but critics of the system have become increasingly vocal. Some of this criticism has come from unusual sources. Steve Jobs, CEO of Apple Computer, recently wrote that "DRMs haven't worked, and may never work, to halt music piracy".

This month, we'll examine how some of the most popular DRM systems work, and the limitations and failures that have seen some prove extremely ineffective.

KNOW YOUR RIGHTS

Not so long ago, the idea of buying music or video files from the internet was laughable. Using a 28.8Kbit/s modem, a music track encoded as a 4MB MP3 file took around 20 minutes to download, and a 12-track album took four hours. The best modems running at 56Kbit/s could halve these times, but two hours is still a long time to wait when each minute of internet access increases your phone bill. DVD video discs can contain up to 8.5GB of data, so downloading one of those could take a little under two weeks. One user might be able to download a handful of music tracks illegally, but the chance of engaging in any wholesale theft of films and music was fairly remote.

With the emergence of cheap, fast broadband internet connections, though, downloading music and video files has become simple and practical. For the companies that distribute

music and film, this is both a blessing and a curse. It makes it simple and cheap to sell music directly to customers, but it also makes it easy for customers who have bought music or films, online or as a CD or DVD, to share them with others who haven't paid. With this in mind, distributors of media files wanted to find a way to sell digital media files that can be played by the buyer, but not by anyone else who might acquire them. The mechanisms that allow this have become known as DRM.

DVD DRAMA

Although DRM is generally associated with online distribution services such as the iTunes Store, the first common application of DRM for music and video use was in the specification for DVD Video discs. Most commercial DVDs are encrypted using a DRM system called the Content Scrambling System, or CSS. CSS was designed to allow anyone with a DVD player to play a DVD Video disc, but to make it difficult for people to copy the film to a computer, recompress it and send the smaller file across the internet. CSS doesn't prevent someone making a verbatim copy of the whole disc and playing that back, but when it was designed the dual-layer discs needed to do this were prohibitively expensive.

The CSS system is based on a set of 409 encryption keys called Player Keys. We'll call these PK1, PK2 and so on up to PK409. Every DVD player, be it a domestic player or a software utility such as WinDVD, contains one or more of these keys. To get a key, anyone making a DVD player needs to pay for a licence from the DVD

Copy Control Association. The video files on a DVD are not encrypted using any of the Player Keys. Instead, they are encrypted using separate keys known as Title Keys. These are stored on the disc, in a file encrypted using a single Disc Key (DK). This key varies from DVD to DVD.

As well as the video files, every DVD has a block of data containing 410 files. Four hundred and nine of these each contain the DK, encrypted with a different one of the Player Keys. The first file contains the Disc Key encrypted using PK1, the second the Disc Key encrypted using PK2, and so on. The final, 410th file is

the data produced when the Disc Key is put through a one-way hash function that is known to the DVD player. Hash functions are a one-way process that converts a string of data, A, to another, B. The values of B produced by a hash function are unique, so if two unknown items of data both produce the value B when put through the same hash function, we know that they too must be identical.

When you insert a disc into the DVD player, it attempts to decrypt the Disc Key using its Player Key value. If it knows PK102, for example, it will attempt to use it to decrypt the 102nd encrypted value of DK. This produces a key, but the player needs to check that it is correct. To do this, it runs it through the hash function. It then compares the result with the hashed value stored in the 410th file on the disc. If the two match, it knows that it has the correct key. It can then decrypt the Title Keys and show the video. If the hashed values don't match, the player will repeat the process with the next encrypted DK value on the disc, and so on until it finds the valid Disk Key or fails altogether.

Using 409 keys sounds overcomplicated, but there was some logic behind this design. The idea was that different keys would be given to different DVD player manufacturers. If one key became public knowledge, this key could be omitted when preparing the encrypted Disc Key values for future discs. Anyone using a pirated key would then be unable to use it. Unfortunately for the DVD industry, a single leaked key proved to be the least of its problems.

HACK ATTACK

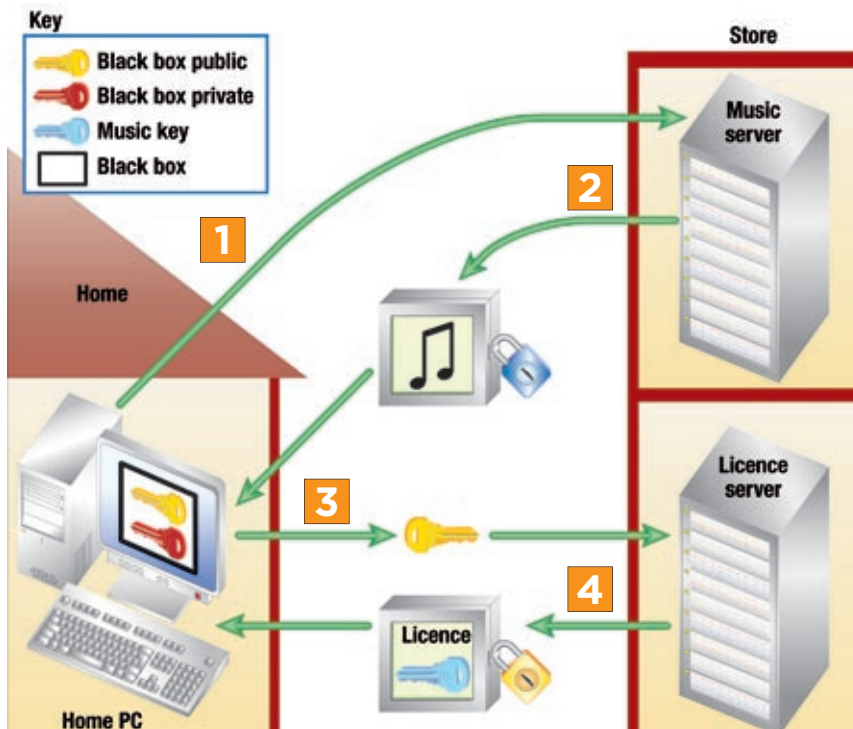
Since its release, the CSS encryption system has been comprehensively broken. Numerous utilities that strip this protection from any standard DVD are easily available. The problems began in 1999 when Xing Technologies, the manufacturer of a software DVD player, neglected to encrypt the Player Key embedded in one of its products, XingDVD. Armed with this one short key, programmers were able to guess around 170 other keys. A small software utility called DeCSS, which used these keys to extract the contents of a CSS-protected DVD, was made available for free on the internet. With almost half of the available keys no longer a secret, removing the compromised keys from future DVDs would have made them unplayable by many DVD players.

Even if one key had not escaped into the hands of programmers, though, it's likely that



▲ Napster uses Windows Media DRM technology to protect the music it hires and sells

Key issues How Windows Media DRM works



▲ When you buy a song protected by Windows Media DRM (Step 1), the encrypted music is downloaded to your PC (Step 2). Your computer's Windows Media Black Box software provides its public key to the online licence server (Step 3), so this can be used to encrypt a licence file that is then returned (Step 4). This file contains the key needed to decrypt and play the song

CSS would have been compromised at some point. The keys it uses for encryption are only 40 bits, or 40 binary digits, long. This means there are 2^{40} (1,099,511,627,776) possible values of a DVD disc key. This sounds impressive, but in reality a 40-bit key is considered relatively weak. RSA security currently recommends that, for data to be considered secure up until the year 2010, a 1,024-bit key should be used. In addition to a brute force attack, where a computer is used to guess keys repeatedly until the correct one is found, analysts located four other weaknesses in the system that could be exploited to circumvent CSS encryption. Today, numerous free tools make it extremely easy for anyone with a computer to decrypt the contents of a DVD, giving them access to the raw video files inside.

CAUGHT NAPPING

The problems of CSS encryption, where an early breach of security left manufacturers unable to secure future releases properly, appear to have influenced the design of more modern DRM systems. Both the major music protection systems, Windows Media DRM and Apple's FairPlay, are capable of being updated should the current encryption system be defeated. To show how they work, we'll examine Microsoft's Windows Media DRM, used by services such as Napster.com, in detail.

The Windows Media DRM system is based on the principle of public key cryptography. We explained the mathematics behind public key cryptography in *How It Works*, *Shopper* July 2006, but the basic principle is simple. Public key cryptography requires two keys: one public and one private. The public key can be freely distributed, while the private key is kept secret by the party that needs to receive information securely. Anybody can encrypt data using the

public key, but it can only be decrypted by the person or device that knows the private key.

To use a Windows Media DRM service, you need some special software on your computer. The software is available only for Windows computers, so stores that use Windows Media DRM can't sell music to those using Apple or Linux computers. The software includes one vital component, known as the Black Box. This contains a public key and a private key, so it can receive information securely. Music files downloaded from a store are encrypted using a separate key, which we'll call the Music Key. The music key can be different for each music file. The music file itself contains no licence or key information, only the encrypted music.

When you attempt to play an encrypted music file, Windows Media Player looks for a licence file on your computer. If you've played the file before, the licence file should be on your hard disk. If you haven't played it before, Media Player needs to acquire the necessary key. To do this, it contacts an online licence server. If this is the first time that you have bought and played a protected song, the licence server will ensure you are a valid user of the service, by prompting for a password for example, then instruct your computer to download a new Black Box. This Black Box contains a new public key, private key and signature, and the service knows it is tied to your user account at the music store. If you've already downloaded and played music, the necessary Black Box will be on your hard disk, so your computer sends its signature and public key back to the licence server to prove that it's present and that it has not been tampered with.

If the licence server is satisfied that your computer has the necessary Black Box, and so belongs to a legitimate listener for the track in question, it sends you a licence file. This file

contains several items of information. One is a content identifier that tells the computer which music or video file it relates to. Another is a digital signature for the licence file.

The final two components are more important, and both are encrypted using the public key of the computer's Black Box. One is the usage rights, which dictate the terms under which the file can be played. A rented movie file might be playable only for a certain period, for example, or a sample music file may be playable only three times. The final part contains the Music Key needed to decrypt the media file.

With the licence file downloaded and stored on the computer, the Black Box checks its digital signature to ensure that the licence has not been tampered with. If it is satisfied that the licence is valid, it uses its private key to decrypt the usage rights and Music Key. If the circumstances in which it is being played are acceptable under the usage rights in the licence, it uses the decrypted Music Key to decrypt the media file, allowing the computer to play it.

LITTLE BOXES

This system sounds complicated, and in some respects it is: in Microsoft's patent application for the technology even a simplified explanation in the form of a flow diagram takes up two pages. However, it has some important advantages over simpler methods. For one, the system is flexible. The usage rights encoded into the licence file for any media item allow the system to protect music that's sold, rented or released for a limited period. With a simpler system such as CSS, this isn't possible – either the DVD player is verified and the disc plays, or it will never play.

More importantly, Microsoft's system is more resilient against security breaches. The many checks built into the process of playing a file give the Black Box and the licence server the chance to detect if one part of the system has been tampered with. And, unlike CSS encryption, the entire system can be updated via the internet. If the entire system is comprehensively breached, vendors can force users who buy new files to download a new Black Box in order to play them. This will protect any new purchases using the new Black Box. In August 2006, a utility called FairUse4WM successfully circumvented the Windows Media DRM system, and Microsoft released a new Black Box to block it. A second version of FairUse4WM emerged, prompting Microsoft to advise its partners that it again intended to patch the hole using a new Black Box. Despite two effective circumventions of the system, stores are able to continue to sell music and video files secured by the system. **CS**

FURTHER INFORMATION

Analysis of CSS and its vulnerabilities
www.dvd-copy.com/news/cryptanalysis_of_contents_scrambling_system.htm
www.cs.cmu.edu/~dst/DeCSS/Kesden/index.html

'Why the DVD hack was a cinch'
www.wired.com/science/discoveries/news/1999/11/32263

Engadget reports a purportedly leaked Microsoft memo regarding the FairUse4WM vulnerability
www.engadget.com/2006/09/25/microsoft-claims-successful-patch-against-fairuse4wm-1-2/